Fog Ransomware: Unusual Toolset Used in Recent Attack

security.com/threat-intelligence/fog-ransomware-attack

Threat Hunter TeamSymantec and Carbon Black

A May 2025 attack on a financial institution in Asia saw the Fog ransomware deployed, alongside an unusual toolset, including some dual-use and open-source pentesting tools we have not observed being used in ransomware attacks previously.

The attackers used a legitimate employee monitoring software called Syteca (formerly Ekran), which is highly unusual and not something we have seen used in a ransomware attack chain before. They also deployed several open-source pentesting tools – GC2, Adaptix, and Stowaway – which are not commonly used during ransomware attacks.

Also notable in this attack was that, a few days after the ransomware was deployed, the attackers created a service to establish persistence. This is an unusual step to see in a ransomware attack, with malicious activity usually ceasing on a network once the attackers have exfiltrated data and deployed the ransomware, but the attackers in this incident appeared to wish to retain access to the victim's network.

The attackers were on the target's network for about two weeks before they deployed the ransomware.

Fog ransomware

The Fog ransomware was first documented in May 2024, and initially appeared to be primarily focused on targeting educational institutions in the U.S. In those early attacks, attackers using Fog gained initial access to networks by leveraging compromised VPN credentials.

It was reported in October 2024 that attackers using Fog were targeting a critical vulnerability (CVE-2024-40711 - CVSS 9.8) in the Veeam Backup & Replication (VBR) servers that was patched in September 2024. Meanwhile, in April 2025, Fog attackers were reported to be using email as an initial infection vector in ransomware attacks in which the language used in the ransom notes appeared to be mocking Elon Musk's Department of Government Efficiency (DOGE) in an effort to goad victims. Also notable in that attack campaign was that the ransom notes also offered a "decrypt for free" option if the victim chose to spread the ransomware to somebody else's computer.

Toolset

The initial infection vector used by the attackers in this recent incident isn't known. Two of the infected machines were Exchange Servers. While there was no evidence to suggest they were the initial infection vector, exploiting vulnerabilities in Exchange Servers is a common initial infection vector for ransomware actors.

The first suspicious activity on the network was the installation of multiple open-source, post-exploitation penetration testing tools, including variants of the GC2 tool, which is an open-source tool that allows an attacker to execute commands on target machines using Google Sheets or Microsoft SharePoint List and exfiltrate files using Google Drive or Microsoft SharePoint documents. The GC2 implant polls the Google Sheet or SharePoint List for each operator command, then uses it to store its output, a log, and records the execution polling interval it is configured with.

It is used by the attackers for various discovery commands.

```
whoami
```

```
net use

cmd /c "ipconfig /all"

cmd /c "netstat -anot|findstr 3389"
```

When communicating with the remote attacker, the GC2 tool also checks for the following commands:

- "exit"
- "load" (added functionality): loads arbitrary file and executes it as shellcode
- "upload"
- "download"

It contains two embedded configuration blobs in encoded form.

This tool is not something we have seen used in ransomware attacks before, though it was used in an attack carried out by Chinese nation-state backed actor APT41 in 2023.

The open-source Stowaway proxy tool was used to deliver the Syteca (formerly Ekran) executable. It is not clear exactly what the Syteca tool was used for by the attackers. In the attack, the file is named 'sytecaclient.exe', but it also appears with the name 'update.exe.' Syteca is legitimate employee monitoring software that can record onscreen activity and monitor keystrokes, among other capabilities.

Several libraries are loaded by this executable, suggesting it was possibly used for information stealing or spying, which would be the most likely reason the attackers would deploy it given the keylogging and screen capture capabilities of the tool.

```
CSIDL_SYSTEM\regsvr32.exe" /s /u [REDACTED] Files\Ekran System\Ekran
System\Client\SoundCapture_7.20.576.0.dll""

CSIDL_SYSTEM\regsvr32.exe" /s /u [REDACTED] Files\Ekran System\Ekran
System\Client\x86\SoundCapture_7.20.576.0.dll""

CSIDL_SYSTEM\regsvr32.exe" /s /u [REDACTED] Files\Ekran System\Ekran
System\Client\CredentialProviderWrapper.dll""

CSIDL_SYSTEM\regsvr32.exe" /s /u [REDACTED] Files\Ekran System\Ekran
System\Client\CredentialProviderWrapper_7.20.576.0.dll""
```

Several commands that look like they are removing or killing the Syteca executable are also executed. This appears to be an attempt by the attackers to delete indicators and evidence of their activity on the network in an effort to avoid detection.

```
CSIDL_SYSTEM\taskkill.exe /f /im "EkranClient.exe"
```

```
CSIDL_SYSTEM\taskkill.exe /f /im "EkranClientSession.exe"

CSIDL_SYSTEM\taskkill.exe /f /im "EkranController.exe"

CSIDL_SYSTEM\taskkill.exe /f /im "grpcwebproxy.exe"

CSIDL_SYSTEM\taskkill.exe /f /im "PamConnectionManager.exe"

CSIDL_SYSTEM_DRIVE\program files\ekran system\ekran
system\tmp\usbdriverinstaller.exe" -u [REDACTED]

CSIDL_SYSTEM_DRIVE\program files\ekran system\ekran
system\tmp\usbolddriveruninstaller.exe
```

PsExec was also used to remove the Syteca client configuration file and binary in another attempt by the attackers to delete evidence of the presence of Syteca on the network:

```
psexec64.exe -accepteula \\192.168.8.52 -u <?,?> -p <?,?> -h -s cmd /c "del
C:\users\public\SytecaClient.ini"

psexec64.exe -accepteula \\192.168.8.150 -u <?,?> -p <?,?> -h -s cmd /c "rm
C:\users\public\SytecaClient.exe"
```

PsExec and SMBExec were also used alongside Syteca and GC2 for lateral movement across the victim network.

SMBExec was used to launch Syteca:

```
cmd.exe /Q /c SytecaClient.exe 1> \\127.0.0.1\ADMIN$\__1748095766.8385904 2>&1
```

PsExec was used to laterally execute a suspected process watchdog/launcher for the GC2 backdoor:

```
psexec64.exe -accepteual \\192.168.8.52 -u <?,?> -p <?,?> -h -s cmd /c
"CSIDL_COMMON_APPDATA\microsoft\devicesync\windowsdevicesync.exe"
```

SMBExec and PsExec are both living off the land tools that are commonly used by ransomware attackers:

- PsExec: Microsoft Sysinternals tool for executing processes on other systems. The tool is primarily used by attackers to move laterally on victim networks.
- SMBExec: Open-source lateral movement tool.

For data theft, the attackers download multiple file transfer utilities - Freefilesync and MegaSync - as well as using 7-zip to archive sensitive directories.

- 7-zip: Legitimate open-source file archiver with a high compression ratio.
- FreeFileSync: An open-source folder comparison and synchronization tool.
- MegaSync: A synchronization tool for the Mega file hosting platform.

Other tools used on the target's network include the Adaptix C2 Agent Beacon, which is a component of an open-source extensible post-exploitation and adversarial emulation framework, Adaptix C2, designed for use by penetration testers. The variant used on the target's network in this incident contained a configuration blob in encrypted form. Adaptix can be considered a sort of open-source alternative to the well-known Cobalt Strike framework. The Adaptix beacon agent is similar to Cobalt Strike beacon; once implanted on a victim machine, it calls back to the attacker and provides command and control (C&C) access.

The attackers also used Process Watchdog, a program that continuously enumerates running processes to check for a specific process, in this case the GC2 process, which has the filename *AppxModels.exe* and, if not found on a machine, Process Watchdog creates the process.

```
C:\ProgramData\Microsoft\Windows\Models\AppxModels.exe
```

On the day the Fog ransomware was deployed, the Impacket SMB tool was also used, suggesting this may have been used to deploy the ransomware.

Notably, several days after the ransomware was deployed, a service was run to establish persistence on the victim network. This is likely another process watchdog used to launch one of the attacker's command and control tools, such as GC2.

```
sc create SecurityHealthIron binPath=
"CSIDL_SYSTEM\diagsvcs\runtimebroker.exe" start= auto DisplayName= "Collect
performance information about an application by using command-line tools."

sc start SecurityHealthIron
```

An unusual ransomware attack

There are a few things that mark this ransomware attack out as unusual. The toolset deployed by the attackers is quite atypical for a ransomware attack. The Syteca client and GC2 tool are not tools we have seen deployed in ransomware attacks before, while the Stowaway proxy tool and Adaptix C2 Agent Beacon are also unusual tools to see being used in a ransomware attack.

The attackers establishing persistence on a victim network having deployed the ransomware is also not something we would typically see in a ransomware attack.

These factors mean it could be possible that this company may in fact have been targeted for espionage purposes, with the ransomware attack merely a decoy, or perhaps also deployed in an attempt by the attackers to make some money while also carrying out their espionage activity.

What we can say with certainty is that this was an unusual toolset to see in a ransomware attack and is worth noting for businesses and corporations wanting to guard against attacks by malicious actors.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.

File indicators

181cf6f9b656a946e7d4ca7c7d8a5002d3d407b4e89973ecad60cee028ae5afa – Fog ransomware

90a027f44f7275313b726028eaaed46f6918210d3b96b84e7b1b40d5f51d7e85 – Process Watchdog

f6cfd936a706ba56c3dcae562ff5f75a630ff5e25fcb6149fe77345afd262aab – Process Watchdog

fcf1da46d66cc6a0a34d68fe79a33bc3e8439affdee942ed82f6623586b01dd1 – Process Watchdog

4d80c6fcd685961e60ba82fa10d34607d09dacf23d81105df558434f82d67a5e – Likely Process Watchdog

8ed42a1223bfaec9676780137c1080d248af9ac71766c0a80bed6eb4a1b9b4f1 – Likely Process Watchdog

e1f571f4bc564f000f18a10ebb7ee7f936463e17ebff75a11178cc9fb855fca4 – Likely Process Watchdog

f1c22cbd2d13c58ff9bafae2af33c33d5b05049de83f94b775cdd523e393ec40 – Likely Process Watchdog

279f32c2bb367cc50e053fbd4b443f315823735a3d78ec4ee245860043f72406 – Likely Process Watchdog

b448321baae50220782e345ea629d4874cbd13356f54f2bbee857a90b5ce81f6 – Likely Process Watchdog

f37c62c5b92eecf177e3b7f98ac959e8a67de5f8721da275b6541437410ffae1 – GC2-sheet

3d1d4259fc6e02599a912493dfb7e39bd56917d1073fdba3d66a96ff516a0982 – GC2-sheet

982d840de531e72a098713fb9bd6aa8a4bf3ccaff365c0f647e8a50100db806d – Likely GC2-sheet

fd9f6d828dea66ccc870f56ef66381230139e6d4d68e2e5bcd2a60cc835c0cc6 – Syteca executable

bb4f3cd0bc9954b2a59d6cf3d652e5994757b87328d51aa7b1c94086b9f89be0 – Stowaway

ba96c0399319848da3f9b965627a583882d352eb650b5f60149b46671753d7dd – Adaptix C2 Beacon Agent

44bb7d9856ba97271d8f37896071b72dfbed2d9fb6c70ac1e70247cddbd54490 – Likely Adaptix C2 Beacon Agent

13d70c27dfa36ba3ae1b10af6def9bf34de81f6e521601123a5fa5b20477f277 – Stowaway

Network IOCs

66.112.216[.]232

amanda[.]protoflint[.]com

97.64.81[.]119

About the Author

Threat Hunter Team

Symantec and Carbon Black

The Threat Hunter Team is a group of security experts within Broadcom whose mission is to investigate targeted attacks, drive enhanced protection in Symantec and Carbon Black products, and offer analysis that helps customers respond to attacks.